I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

China in Global Trade: Proposed Data Protection Law and Encryption Standard Dispute

AIMEE BORAM YANG*

Abstract: The remarkable growth of China's economy has made it an attractive trade partner. However, to flourish as an attractive trade partner, China must first settle two critical, yet unresolved global trade issues: the new privacy governance regime and the encryption standard system. This note first addresses the recent updates on the proposed data protection law in China and key issues to consider before enacting and implementing the new law. Today, the data protection law is a key issue in modern business practices because many businesses are information-oriented, frequently involving data processing and thus requiring appropriate protection regulation. Unlike the European Union, which is governed by the E.U. Data Protection Directive, Asia does not currently have a unified data protection law. However, in some jurisdictions in Asia, data protection law is slowly developing and China is one of them.

In a global world, and particularly with China as one of the leading economies, data protection law in China is a critical issue because without such law, many multinational businesses trading with China are exposed to various privacy risks stemming from lack of transparency and data manipulations. China began drafting the data protection law in 2003, and completed it in 2005, but the law was not implemented. Today, China is preparing a new personal

* The author is a Juris Doctor Candidate at The Ohio State University Moritz College of Law, Class of 2009. She obtained a Masters of International Studies in International Business from the Graduate School of International Studies at Ewha Womans University, where she also received a B.A. in English Language and Literature and a minor in Chinese Language and Literature.

data protection law, based on the 2005 draft, that will avoid compromising the country's economic growth. Because the draft has yet to be included on China's legislative agenda, it will take some time to become a law; however, under the recently reorganized Ministry of Industry and Information Technology, it is expected to be enacted in the near future.

This note also presents an overview of the controversy surrounding international encryption policy and the encryption standard dispute between China and foreign software companies. Although the global encryption standard is 802.11 standard by IEEE, in 2003, China has announced WAPI, its own encryption standard as a required encryption standard for all Wi-Fi systems sold in China. The new standard brought intense dispute between the foreign software companies and China because one, it was seen as an unfair trade barrier to sales and, two, the WAPI standard would have forced foreign companies to cooperate with a number of Chinese companies by licensing the WAPI technology. Due to growing concerns and criticisms, China finally announced to indefinitely delay the implementation of WAPI.

I. INTRODUCTION: CHINA IN GLOBAL TRADE

Qing ren yan li chu xi shi– beauty is in the eye of the beholder. Despite growing concerns about the lack of privacy and data protection measures, and significant frustrations over trade barrier-like encryption standards, today China still stands as a leader in global trade. This is true not only because China has an advantageous location for outsourcing due to its low-cost labor force, but also because of the potential consumers in China's middle class of 100 million people.[1] To capture these benefits, information must continue to flow in and out of China so that international companies can ensure that their employees in China have access to data necessary to carry on their job functions.[2] Also, businesses need the ability to send information to China to facilitate business processes and to collect, analyze, and share data about consumers to better understand the Chinese consumer market.[3]

II. NEW DATA PROTECTION LAW IN CHINA

A. GLOBAL PRIVACY FRAMEWORKS

Privacy has been defined using various concepts and terms. In 1997, the United Kingdom's Calcutt Committee defined privacy as "[t]he right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information."[4] Today, a vast amount of information passes over the Internet without regard for national borders.[5] Such borderless flow often involves multi-jurisdictional

---

[1] THE CTR. FOR INFO. POL'Y LEADERSHIP, HUNTON & WILLIAMS LLP, CHINA PRIVACY GOVERNANCE (June 2007), http://www.hunton.com/files/tbl_s47Details/FileUpload265/1944/China_Privacy_Two-Pager.pdf.

[2] *Id.*

[3] *Id.*

[4] PETER P. SWIRE & SOL BERMANN, INFORMATION PRIVACY 1 (Peter Kosmala ed., International Association of Privacy Professionals 2007) (citing Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE L.J. 421, 428 (1980)).

[5] Manuel E. Maisog, *Prospects for a Personal Information Protection Law*, 21 CHINA L. & PRAC. 65, 65 (Sept. 2007).

issues of privacy law; therefore, the privacy laws of several nations must be considered together because they are interrelated in protecting the privacy of personal information sent over the Internet.[6]

Jurisdictions that have a privacy law framework vary in terms of the data protection models they have implemented.[7] The United States's framework is industry-specific and supportive of self-regulation; Europe, on the other hand, has data protection laws that are comprehensive, centralized, and enforced by national regulators.[8] Canada and Australia have co-regulatory models where industry creates standards for privacy that are enforced by the industry and overseen by a private agency.[9] Japan has a self-regulatory model somewhat similar to the United States's model; however, Japan requires companies to abide by codes of practice set by a company, group of companies, industry bodies, or independent bodies.[10]

In June 2006, the Chinese Academy of Social Sciences ("CASS")[11] and Acxiom China[12] hosted a symposium on the development of Chinese privacy law.[13] At that meeting, numerous government

---

[6] *Id.*

[7] SWIRE & BERMANN, *supra* note 4, at 4–5.

[8] EU-China Info. Soc'y Project, *Workshop on "Data Protection Issue Identification,"* http://www.eu-china-infso.org/Regulation/regulation090800@2007-04-20.html (last visited Feb. 7, 2009); Bridget Treacy, *Current Data Protection Issues for Financial Institutions*, 7 PRIVACY & DATA PROT. 3, 4 (2007), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1963/data_protection2_B.Treacy.pdf.

[9] SWIRE & BERMANN, *supra* note 4, at 5.

[10] *Id.*

[11] CASS is the highest academic research organization for the social sciences and is also a national center for comprehensive studies in China; it is affiliated to the State Council of China. Chinese Academy of Social Sciences, http://bic.cass.cn/English/InfoShow/Arcitle_Show_Cass.asp?BigClassID=1&Title=CASS (last visited Feb. 7, 2009); Wikipedia, Chinese Academy of Social Sciences, http://en.wikipedia.org/wiki/Chinese_Academy_of_Social_Sciences (last visited Feb. 7, 2009).

[12] Acxiom China is a wholly owned subsidiary of Acxiom Corporation in China, which provides data management services and data to the private sector and to other organizations to allow them to achieve more effective customer information management and to minimize risk. More information on Acxiom is available on their website at http://www.acxiom.com.cn/?displayid=116 (last visited Feb. 7, 2009).

officials, members of academia, and business representatives shared their experiences with privacy and data protection law in the Americas, Europe and Asia, and formulated issues that a Chinese privacy law should address. [14] The discussion illuminated the complexity of drafting privacy laws in China because China does not necessarily seek an American or European approach, but instead focuses on developing a solution that will not impact its economic growth.[15]

At this time, it is difficult to identify which model China will eventually adopt. However, it is interesting to note that the initial 2005 draft of China's privacy laws[16] was heavily influenced by both the Asia Pacific Economic Cooperation ("APEC") [17] and the European Union frameworks. [18] Even more significantly, recent opinions indicate that the new Chinese law will likely take an approach similar to Japan's, [19] and thus it now appears China may adopt a self-regulatory model or at least a model based primarily on self-regulation.

B. PRIVACY FRAMEWORK AND CHINA

In contrast to Western culture, where the concept of privacy is deeply rooted, Chinese culture has had no tradition of privacy;

---

[13] *Update on Development of China's Privacy Law*, CLIENT ALERT (Hunton & Williams LLP, New York, N.Y.), July 2006, http://www.hunton.com/files/tbl_s10News/FileUpload44/13337/ChinaPrivacyLawAlert.pdf.

[14] *Id.*

[15] *Id.*

[16] *See infra* Section II.C.

[17] The Asia Pacific Economic Cooperation ("APEC") is a multi-national organization with members in Asia and the Americas. The APEC Privacy Subgroup developed the APEC Privacy Framework that provides support to "APEC-member economic legislation that would protect individual interests and ensure the economic development of all APEC member economies." SWIRE & BERMANN, *supra* note 4, at 97.

[18] Treacy, *supra* note 8, at 4. The European Union passed the E.U. Data Protection Directive, the European Union's comprehensive law to protect the fundamental rights and freedoms of E.U. citizens, particularly their right to privacy in personal data processing. SWIRE & BERMANN, *supra* note 4, at 84.

[19] Telephone Interview with Martin. E. Abrams, Senior Policy Advisor and Executive Director, Ctr. for Info. Pol'y Leadership, Hunton & Williams LLP (Mar. 19, 2008).

therefore, the concept of "privacy" or "personal information" is new to many people in China. [20] This is true mainly because China's communist government keeps personal records on every citizen. [21] The government's invasiveness was most severe under Mao Zedong, when the government "controlled all jobs, housing and services through the household registration system."[22] Thus, it is no surprise that the issue of personal privacy is controversial in China. However, this cultural difference between China and Western nations does not mean that privacy remains entirely foreign to Chinese culture. Chinese society has transformed since the times of Mao Zedong's government controlling every citizen. Economic reforms have brought financial independence for many citizens, and notably, rising wealth has led to demands for private property and has expanded the Chinese people's sense of what should be regarded as private.[23] As a result, numerous debates about the meaning of privacy, growing concerns over privacy infringement, and extensive preparation of data protection law are all slowly framing the concept of privacy in China.

China still does not have clear legal provisions to protect privacy or data. As of a June 1, 2008 estimate, China had the largest number of regular Internet users in the world, with over 300 million.[24] The lack of protective measures has led to a remarkable increase in the misuse of personal information and has put the personal information of millions of people at risk of future abuse. [25] Advertisers, especially, have been guilty of exploiting personal information of Chinese citizens for gain. For example, today in China it is not surprising to find a new

---

[20] *See* Treacy, *supra* note 8, at 4 ("Until recently, there was no word in the Chinese language to describe the Western concept of 'privacy.'").

[21] Owen Fletcher, *Chinese Fear Online Mobs*, ASIA TIMES ONLINE, Sept. 25, 2008, http://www.atimes.com/atimes/China/JI25Ad01.html.

[22] *Id.*

[23] *Id.*

[24] Yu Du & Matthew Murphy, *Data Protection and Privacy Issues in China*, HG.ORG, http://www.hg.org/article.asp?id=5340 (last visited Feb. 7, 2009).

[25] *See China Drafts Law to Protect Personal Information*, CRIENGLISH.COM, Jan. 9, 2006, http://english.cri.cn/2238/2006-1-9/51@292261.htm (Individual privacy was seriously infringed when a Chinese website publicly put nine thousand pieces of personal data on sale, including private phone numbers, addresses, and financial records.); *Huge Concerns Over Access to Private Details*, CHINA DAILY, June 6, 2006, http://www.china.org.cn/english/2006/Jun/170550.htm (90 million people's detailed personal data were accessible at a Chinese website, "Souren" or "personal search.").

mother flooded with milk powder advertisements the day after she gives birth to a child.[26] Despite such risks and harms, however, in the absence of clear data protection laws, victims cannot protect themselves through lawsuits.[27]

Many people blame the Chinese government and hold it responsible for putting their private information in peril.[28] Thus, Chinese lawmakers and citizens have been urging their government to speed up the enhanced legislation that will restrict rampant privacy infringement and designate personal data as private information.[29]

Because protecting privacy has not been a part of tradition in China, when the new law was finally proposed, there was extensive debate about whether the proposed law should be limited to the protection of personal data, or whether the law should cover privacy in broader terms.[30] Personal information protection law, which is often called "data protection law" is "law that governs the collection, storage, processing and use of information relating to a living natural person from which, it is practicable to ascertain the identity of that person."[31] Such information typically includes "personal information," such as an individual's identification card, credit card and bank account numbers, private address, and passport number.[32]

More recently, the debates in China have focused on the implementation of a framework to protect personal information,

---

[26] Zhu Zhe, *Law on Personal Info 'Next Year,'* CHINA DAILY, Aug. 6, 2007, http://www.chinadaily.com.cn/china/2007-08/06/content_5448419.htm.

[27] *See China Drafts Law to Protect Personal Information*, *supra* note 25.

[28] *See Huge Concerns Over Access to Private Details*, *supra* note 25.

[29] *Lawmaker Urges Legislation to Curb Rampant Privacy Infringement*, XINHUA NEWS AGENCY, Mar. 6, 2005, http://www.china.org.cn/english/2005lh/121920.htm (In 2005, a deputy to the National People's Congress, a top legislature in China, proposed an earlier enactment of a law to protect citizens' personal information. Also, a Chinese lawyer pointed out that a privacy law should protect anything that relates to the privacy of a citizen.); *see Huge Concerns Over Access to Private Details*, *supra* note 25 (In 2006, according to a national survey, 91.8% of Chinese people were concerned that their private details had been leaked and used illegally; another 74% believed China needed tougher laws to protect privacy.).

[30] EU-China Info. Soc'y Project, *supra* note 8.

[31] Maisog, *supra* note 5.

[32] *Id.*

rather than a framework for privacy in general.[33] This shift in focus is due to various initiatives from specific interest groups, particularly the financial services and telecommunications sectors, which are increasingly concerned about protecting personal information.[34] In 2006, the State Council, China's cabinet, finally launched legislation to protect personal information. The draft law stipulated that because personal information is a citizen's "intangible property," those who use others' personal information for financial gain will be punished for a violation of the law.[35]

At present, the Chinese government seems to be preparing for the "development of a personal data protection regime that is in line with international requirements for data processing and data security and that will allow for reliable and secure transactions in the growing fields of e-government and e-commerce."[36] However, implementing a personal data protection law in China will be a major challenge because the government needs to create "a framework that safeguards

---

[33] Treacy, *supra* note 8, at 4.

[34] *Id.* Fletcher, *supra* note 21 (Many of China's more than 600 million mobile phone users called for protection of their personal information because it was common for businesses to sell clients' contact information. Mobile users have reported that they have received remodeling service advertisements right after buying an apartment. Also, a growing fear from the rise of cyber manhunts added urgency to passing legislation protecting personal information. Such urgency can be seen through an online survey conducted by China Youth Daily in June, 2008, which provides that "20% of respondents feared being targeted by the online mob" and also that 80% "supported stronger regulation of cyber manhunts." One example of cyber manhunt in China would be Wang Fei's case. After discovering Wang Fei's affair, his wife committed suicide and her journal reflecting her anger was posted online by her friend. Within days after the journal was posted, Wang's name, address, phone and national identification numbers appeared online next to his pictures by angry Internet users. This was through a cyber relay in the search for information; so when someone provides the first information, the second person could add a bit more and so on until the information seems complete. The Internet users had begun to harass him by calling him and his company, which soon fired him and his lover. His parents found accusations of murder on their door. Wang sued the major Internet portals "for defamation and for violating his privacy through online postings" and a Beijing court accepted the case, which was the first anti-"human flesh search" lawsuit in China. The outcome of Wang's case could have some effect on the government's consideration in dealing with new demands for privacy rights but many scholars and officials are not clear how strongly the government will regulate the abuse of personal information.).

[35] *China Drafts Law to Protect Personal Information*, *supra* note 25.

[36] EU-China Info. Soc'y Project, *Research Final Workshop: "Personal Data Protection,"* http://www.eu-china-infso.org/Regulation/regulation094158@2007-06-20.html (last visited Feb. 7, 2009).

individuals from harm caused by the misuse of personal information," but at the same time, "does not overly stifle economic activity dependent on such information flows."[37] Such balance is important because restrictions that are too stringent may threaten businesses' ability to use personal information efficiently.[38]

In China, "whether and to what extent to allow personal information to enter China, to be processed in China, and to be transferred to places outside of China" is an important element in national policy.[39] A data protection law would not only significantly affect China's economy and its potential as a destination for the international flow of information, but it could also have a considerable effect on the multinational companies that work with and in China.[40] Should a law be enacted, specific and detailed questions regarding data protection issues, such as whether Chinese banks and credit card issuers will be able to offer financial products and services to compete with those of foreign banks, will arise.[41] The answers to these questions will depend on the content and direction of the law.

Undoubtedly, the data protection law will directly affect multinational companies that process data in China because questions, such as how the data processing should proceed or whether the same information may be transferred to destinations outside of China and be processed there, will all be subject to the regulatory requirements of the law.[42] In fact, data processing functions in China are already affected by the question of whether personal information from other countries may be transferred to China for processing. Under the European Union Data Protection Directive,[43] no data may pass

---

[37] Maisog, *supra* note 5.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id. See* Edmund Sanders, *Consumers Can't Bank on Privacy Protection*, L.A.TIMES, June 22, 2001, at C1, *available at* http://articles.latimes.com/2001/jun/22/business/fi-13335 (Without a proper data protection law, some banks and credit card issuers may disclose their customers' names, addresses, Social Security numbers, and account information to outside firms engaged with financial products such as car insurance, credit cards, mortgages, etc.– even when the customers have opted out of having their information shared with third parties.).

[42] Maisog, *supra* note 5.

[43] Treacy, *supra* note 8, at 4–5.

between a European Union nation and another country unless the European Union recognizes that country's data protection system as "adequate."[44] Thus, China must ensure that its data protection laws will meet the European Union's standards so that China may transfer data to and from the European Union.

Because the Chinese economy is experiencing exponential growth, a balanced privacy framework is critical to China's economic success. The privacy framework in China must protect information flows, respond to consumers and comply with appropriate laws, but must not compromise "the ability of companies that use data to deliver services and create economic value."[45]

C. THE DEVELOPMENT OF NEW PERSONAL DATA PROTECTION LAW AND RELATED ISSUES

1. THE DEVELOPMENT OF NEW PERSONAL DATA PROTECTION LAW

In 2003, China's former State Council Informatization Office ("SCITO"), which is now integrated into the newly formed Ministry of Industry and Information Technology ("MIIT"),[46] entrusted drafting of information laws to the experts at the CASS.[47] In 2005, CASS finished drafting the first version of China's data protection law; the first draft was a proposed personal information protection law.[48]

---

[44] Treacy, *supra* note 8, at 5. Among the privacy laws of various countries, the E.U. Directive is particularly important because it imposes special restrictions on data transfers to a non-European Union country unless the recipient country has an "adequate level" of data protection. SWIRE & BERMANN, *supra* note 4, at 84–85.

[45] THE CTR. FOR INFO. POL'Y LEADERSHIP, *supra* note 1, at 1.

[46] Bridget Treacy & Martin Abrams, *A Privacy Law for China?*, COMPLINET.COM, May 29, 2008, http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C2269%5Cprivacy_law_for_China.pdf; China Int'l Elec. Commerce Network, *Ministry of Industry and Information Technology Inaugurated*, June 30, 2008, http://en.ec.com.cn/article/enindustry/entelecom/enitnews/200806/626052_1.html.

[47] GALEXIA, ASIA-PACIFIC REGION AT THE PRIVACY CROSSROADS (2008), http://www.galexia.com/public/research/assets/asia_at_privacy_crossroads_20080825/asia_at_privacy_crossroads-Appendix.html#Heading18 (citing *China to Legislate for Protection of Personal Information*, PEOPLE'S DAILY ONLINE, Jan. 25, 2005, http://english.peopledaily.com.cn/200501/25/eng20050125_171801.html).

[48] Zhe, *supra* note 26.

Although the initial draft was completed in 2005, it was not implemented; [49] according to an article in the *China Daily* that appeared in August 2007, SCITO prepared and submitted a draft for a new personal information protection law to the Legislative Affairs Office of the State Council.[50] This planned law banned "any entity from disclosing personal data to third parties without the consent of individuals and specifies that they have the duty to ensure the data in their possession is not misused;" however, such information may be disclosed in certain circumstances, such as criminal, tax or media investigations.[51]

While the 2005 draft was not implemented, it served as a foundation for the proposed personal information protection law in 2007.[52] The 2005 draft of the new personal data protection law[53] appears to have been strongly influenced by both the APEC Privacy Principles and the European Union's data protection framework.[54] The proposed law "seeks to govern the processing of personal data by both the public and private sectors and contains familiar obligations and restrictions, including limits on the collection, use and cross-border transfer of personal data."[55] Also, the draft "gives individuals the right to apply to obtain personal information relating to them and to require the correction or cessation of use of any false or inaccurate personal information, but it stops short of providing a right of informational self-determination as such."[56]

The 2005 draft presents some issues that need to be resolved, such as registration, restrictions on data transfers, and regulatory

---

[49] GALEXIA, *supra* note 47.

[50] *Id.* at 65; Telephone Interview with Martin E. Abrams, *supra* note 19.

[51] Agence France-Presse, *China to Introduce Law on Personal Data Protection*, INQUIRER.NET, Aug. 6, 2007, http://newsinfo.inquirer.net/breakingnews/world/view/20070806-80846/China-to-introduce-law-on-personal-data-protection.

[52] GALEXIA, *supra* note 47.

[53] *Id.* The 2005 draft includes a protection list for personal mobile phone numbers, medical files, property documents, etc.

[54] Treacy, *supra* note 8, at 4.

[55] *Id.*

[56] *Id.*

authority.[57] The registration requirement that all users of personal information must register with agencies in charge of information resources imposes significant burdens on private companies. Under this requirement, data users would have to disclose their purposes, contents, methods of collection, and even the security protection measures for the information.[58]

The draft permits restrictions on the conduct of cross-border transfers of personal information by private sector users where the recipient country "cannot give sufficient legal protection towards the personal information."[59] But the "sufficient legal protection" standard is not defined, and even if such a standard were defined, it would likely impede transfers of data to destinations outside of China.[60]

The 2005 draft failed to assign a regulatory authority to supervise the new data protection law.[61] The draft gives responsibility to "government agencies in charge of information resources," without specifically defining any government agency.[62] The impact of the law may significantly differ depending upon which government body oversees its implementation and enforcement.[63] Moreover, without a clear indication of a controlling agency, unnecessary competitions and tensions may arise among different Chinese governmental bodies over which should interpret and enforce the law.[64]

Currently, because the legislative process required for the draft to become law, it is premature to provide an accurate and definitive assessment of the new law.[65] However, based on the 2005 draft, there are prospects for some of the key issues that will likely need to be considered prior to enacting and implementing the new law.

---

[57] Maisog, *supra* note 5.

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *See id.*

[62] *Id.* (The possible government agencies include ministries, commissions, and agencies).

[63] *Id.*

[64] *Id.*

[65] *Id.*

2. THE KEY ISSUES OF THE NEW PERSONAL DATA PROTECTION LAW

When drafting a data protection law, the drafters should consider some general issues, including how to define and deal with sensitive personal data; what to do about the sharing of personal data; whether, and to what extent, the desired result could be achieved by means other than legislation; and so forth.[66] Then the drafters should address some important specific issues that will eventually determine the final framework of the personal data protection law.[67]

First, in order to continue China's remarkable economic and trade growth, the new law must balance the protection of personal data with businesses' needs to use personal data.[68] In order to achieve this objective, lawmakers may want to learn and understand other models that are less heavy on regulation before enacting a law, so that they can enact a data protection law that protects consumers without stifling economic growth or innovation.[69]

Second, China's cultural concept of privacy differs from that of the West, creating a fundamental divide between the underlying principles of the privacy directives in each part of the world. To resolve this issue, China could either adopt Western culture's concept of privacy, or it could separate the concept of *personal information* protection law from the general privacy law and enact a law that focuses on consumer protection.[70]

Third, the international transfer of personal data is an important issue.[71] For instance, China should have in place an "adequate level" of data protection to comply with the E.U. Data Protection Directive, so that China may promote the freer flow of data between China and Europe.[72] However, this would be a challenging objective, because in practice, the European Union has found that only a few countries

---

[66] EU-China Info. Soc'y Project, *Workshop on "Data Protection Issue Identification,"* *supra* note 8.

[67] *Id.*

[68] *Id.*

[69] Maisog, *supra* note 5.

[70] *Id.*

[71] EU-China Info. Soc'y Project, *Workshop on "Data Protection Issue Identification,"* *supra* note 8.

[72] Treacy, *supra* note 8, at 4–5.

achieve such an "adequate level" of data protection. [73] As an alternative objective, China may strive to achieve "interoperability" with the legal regimes of other nations so that personal information can be smoothly transferred in and out of China.[74]

Fourth, Chinese lawmakers have been made aware that the registration requirement imposes serious risks and burdens on data users without providing any benefit of protecting the personal information. As of February 2009, Chinese lawmakers have yet to acknowledge these risks, and it is unclear how they will address and resolve this issue in the new law.[75]

Fifth, the creation of an entirely new central-level agency to mandate the implementation and enforcement of the new law may provide an answer to the question of which government agency is to be in charge of the new law.[76]

D. PROSPECTS FOR THE NEW PERSONAL DATA PROTECTION LAW

At the time of this writing, it is unclear when China will enact the data protection law because it may depend upon the new Ministry's legislative priorities, particularly given the circumstances of the new MIIT formed in 2008.[77] In 2007, one of the original CASS drafters speculated that the new law would be enacted "next year," or in 2008, although, he conceded it might take longer to resolve the details of the proposed law; by the time it was 2008, there was another speculation that the law would be enacted "at some point in the next five years."[78]

---

[73] Maisog, *supra* note 5, at 66 (Only a few countries have achieved an "adequate level" of data protection, including Canada, Argentina, and the U.S. safe harbor system.).

[74] *Id.*

[75] *Id. See* Maisog, *supra* note 5 and accompanying text on registration requirement.

[76] Maisog, *supra* note 5. However, this may also create additional concerns, such as whether the new agency will have sufficient resources to cover all matters, and whether the law will be enforced by the central agency or by provincial offices. Currently, the provincial enforcement is standard in China, but this may change due to the borderless nature of information flows. *Id.*

[77] *China to Consider Measure to Increase Protection of Personal Information*, CLIENT UPDATE (Hunton & Williams LLP, New York, N.Y.), Jan. 2009, http://www.hunton.com/files/tbl_s10News%5CFileUpload44%5C15919%5Cchina_personal_information_1.09.pdf.

[78] Zhe, *supra* note 26; Treacy & Abrams, *supra* note 46.

Despite these speculations, it is unlikely that the law will be passed in the immediate future.[79] This is because the Chinese legislature has not yet determined how the law will be enforced or enacted, and "given the wider global debate that seeks cross-border solutions to data protection regulation, the drafters of the Chinese law may still feel that they need more time to consider their approach."[80]

However, there was conjecture in 2008 that the law would be included in the five-year legislative agenda of the Standing Committee of the National People's Congress ("NPC")[81] in 2009.[82] However, even after the law is added to the legislative agenda, the draft may still need to undergo changes before the Standing Committee makes its revisions, making it an unlikely prospect that the legislature will enact the law in 2009.[83]

Once a proposed law is added to the NPC legislations plan, it still must pass through considerable legislative red tape before the NPC can vote to enact the proposed law. After the draft law is enlisted onto the legislative agenda of the Standing Committee of the NPC,[84] members of the Standing Committee must read the draft several times before they prepare a final version.[85] Members of the standing committee who prepare the final version of the prospective law then present the final version to the Standing Committee as a whole or directly to the NPC.[86] Normally, a data protection law is complex and abstract, therefore, those with knowledge of the Chinese legislative

---

[79] Treacy & Abrams, *supra* note 46.

[80] *Id.*

[81] National People's Congress is the "highest state body and only legislative house" in China. Wikipedia, National People's Congress, http://en.wikipedia.org/wiki/National_People%27s_Congress (last visited Feb. 7, 2009).

[82] Treacy & Abrams, *supra* note 46.

[83] *See* Maisog, *supra* note 5.

[84] PARLIAMENTARY CENTRE, THE LEGISLATIVE PROCESS IN CHINA 1, http://www.parlcent.ca/asia/Docs/China/Attachment/Legislative_process%20in%20China-English.pdf (last visited March 27, 2009) ("The Standing Committee of NPC is in charge of making and revising the other laws except those promulgated by NPC and while NPC is not in session; the Standing Committee is also in charge of supplementing and amending parts of the laws promulgated by NPC.").

[85] *Id.* at 5 (noting that under normal circumstances, bills are examined three times at the standing committee meeting before they are put to vote).

[86] Maisog, *supra* note 5.

process hypothesize that the process may not be completed for several years.[87]

However, if there is a strong consensus about the law, then there is greater possibility that the law could be enacted much sooner.[88] This is because, in China, laws and regulations can be enacted through many different channels.[89] For instance, besides the NPC, the State Council could enact an "administrative regulation" at any time before the NPC or its Standing Committee does so.[90] If the Standing Committee senses that the need for a new personal data protection law is urgent, it may move more quickly, despite its internal review process.[91]

After the revised draft of the law is discussed at the Standing Committee meeting, "the Law Committee revises it and submits a final draft of the law to the Chairperson's Council who submits it to the plenary session of the Standing Committee for voting."[92] Over half of the members of the Standing Committee must pass the draft before it can be adopted as law.[93]

In fashioning a remedy to the privacy debate, China requires a privacy governance regime that plays multiple roles. It should seek to develop a structure that is culturally appropriate in China, and it should protect consumers and their personal information.[94] Simultaneously, however, it should avoid restrictions on global data flows so that the normal flow of information is not disrupted.[95] Lastly,

---

[87] *Id.*

[88] *Id. But see* EU-China Info. Soc'y Project, *supra* note 8. The difficulty of achieving a consensus among the interested parties on the new law is one of the key issues of discussion. *Id.* If all the sides have the same opinion, bills that have been listed on the agenda of the standing committee meeting can be discussed twice at the standing committee meeting before being put to a vote, and if all the sides reach a consensus, some bills can be discussed just once before being put to a vote. PARLIAMENTARY CENTRE, *supra* note 84, at 7.

[89] Maisog, *supra* note 5.

[90] *Id.*

[91] *Id.*

[92] PARLIAMENTARY CENTRE, *supra* note 84, at 8.

[93] *Id.*

[94] THE CTR. FOR INFO. POL'Y LEADERSHIP, *supra* note 1, at 1.

[95] *Id.* Zhe, *supra* note 26.

it should promote a privacy regime that could serve as a model for other Asian countries.[96]

III. ENCRYPTION STANDARD DISPUTE BETWEEN CHINA AND FOREIGN COMPANIES

A. TECHNICAL DISPUTE OVER ENCRYPTION STANDARD

In December 2003, the Beijing government officially introduced a new Chinese domestic wireless local area network ("WLAN") [97] standard, called WLAN Authentication and Privacy Infrastructure ("WAPI")[98] and mandated WAPI for all Wi-Fi systems[99] sold in China, while restricting access to the encryption technology to twenty-four Chinese companies.[100] WAPI was incompatible with the Institute of Electrical and Electronics Engineers ("IEEE") 802.11 technology[101] used in most wireless products. Therefore, given the popular recognition of the 802.11 series as a global standard,[102] a serious encryption standard dispute between the 802.11i standard and China's

---

[96] THE CTR. FOR INFO. POL'Y LEADERSHIP, *supra* note 1, at 1.

[97] A WLAN "is a local-area network in which digital devices communicate through a wireless medium such as radio or fiber-optic cable;" "most WLAN equipment today is based on the IEEE's 802.11 series of standards, known as Wi-Fi technology." MBN Systems, http://www.mbnsystems.com/equipment.htm (last visited Apr. 10, 2009).

[98] Mike Clendenin, *WAPI Battle Exposes Technology Rifts with China*, EE TIMES, Mar. 17, 2006, http://www.eetimes.com/news/semi/showArticle.jhtml?articleID=183700631 (IWNComm, a Chinese company, has developed WAPI and the China Broadband Wireless Internet Protocol Standard Group ("BWIPS") oversees the development of WAPI.).

[99] *See infra* Section III.C.

[100] Clendenin, *supra* note 98.

[101] IEEE's 802.11 standards govern wireless networking transmission methods and are commonly used in their 802.11a, 802.11b, and 802.11g versions to provide wireless connectivity. *See* MBN Systems, *supra* note 97.

[102] Bradford C. Brown, *On The Horizon: Joining WTO Means Playing By Global Rules*, INFORMATIONWEEK, Apr. 5, 2004, http://www.informationweek.com/news/management/showArticle.jhtml?articleID=18700337 (According to the Wi-Fi Alliance, "[m]ore than 1,000 products have supported the 802.11 standard since 1999, and many wireless networks in homes and businesses use products based on it.").

WAPI quickly developed.[103] It may have begun as an encryption standard dispute, but as China's insistence on its own encryption standard continued despite a growing criticism from much of the world, it quickly became a larger trade dispute between China and foreign companies, which were clearly concerned with China's domestic protectionist policy.[104]

B. ENCRYPTION POLICY BATTLE

Data encryption is a technology for effectively scrambling data so that the code cannot be broken and the content cannot be decoded without a digital key.[105] It is used to protect data communications, commercial transactions, and personal records. [106] Encryption technology offers both benefits and risks by protecting the security and integrity of personal and business communications and by allowing criminals to conceal communications about their illicit activities.[107] Accordingly, the U.S. government has had long policy debates over American-made strong public key encryption technology, with one side favoring protection for national security and the other arguing for protection of private communications from government intrusion.[108]

Encryption is subject to regulations around the world because countries view encryption as "dual-use technology": it has both

---

[103] Clendenin, *supra* note 98.

[104] *See* Dan Jones, *Chinese Security Snafu Looms*, UNSTRUNG, Dec. 22, 2003, http://www.unstrung.com/document.asp?doc_id=45257 (At least one analyst has accused China of "enforcing 'protectionist' policies aimed at shoring up market share for domestic vendors.").

[105] Jeri Clausing, *U.S. Losing Battle on Control of Data Encryption, Study Says*, N.Y. TIMES, Feb. 9, 1998, http://query.nytimes.com/gst/fullpage.html?res=9A05E6DE1E3DF93AA35751C0A96E958260.

[106] *Id.*

[107] Michael A. Vatis, *The Value of Understanding International Encryption Regulation*, http://www.steptoe.com/assets/attachments/3423.pdf (last visited Feb. 7, 2009).

[108] Regina Burch, *The Battle Over Encryption Software Export Laws*, 4 CARDOZO ELEC. L. BULL. 6, 7 (Dec. 17, 1997), *available at* http://www.jus.unitn.it/Cardozo/Review/Informatica/Burch-1998/Encrypt.html; *see* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT SAVING PRIVACY IN THE DIGITAL AGE (Penguin 2002).

military and commercial value.[109] Many countries have developed their own controls and sanctions for data security and the use of encryption technology, and they set restrictions on its import, export, and use.[110] By classifying encryption as "munitions," the U.S. government had, until recently, tightly controlled the export of advanced encryption software that was capable of reading encrypted messages necessary for national security or law enforcement purposes.[111] Near the end of the Clinton Administration, many of the restrictions were loosened, which was a particular relief for American software companies who found the strict regulations an obstacle to their ability to compete globally.[112]

Multinational coordination among governments is needed for a global information infrastructure to be effective. But, some countries have developed their own policies that are vastly different from other governments, making coordination near impossible.[113] Strong encryption technology in the world market presents problems.[114] If the encryption is unbreakable, then a government has to go to the developer to obtain the source code every time it needs to decode a message for law enforcement purposes.[115] Moreover, this would allow private industry to participate in decisions of how to investigate and prosecute criminals.[116] This would result in high transaction costs borne by law enforcement, and would place a heavy burden on the encryption software industry to continuously provide the source code to governments throughout the world.[117]

---

[109] Ellen Messmer, *Encryption Restrictions*, NETWORK WORLD, Mar. 15, 2004, http://www.networkworld.com/careers/2004/0315man.html?page=1.

[110] *Id.*

[111] T.K. Chang, *Security vs. Liberty in the Information Age*, ASIAN WALL ST. J., Feb. 22, 2000, http://www.angelfire.com/stars/tkchang/Security_vs_Liberty.htm.

[112] *Encryption Export Rules Eased*, CNET NEWS, May 8, 1997, http://www.news.com/2100-1001-279620.html.

[113] Burch, *supra* note 108.

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

Thus, in order to maintain a balance between national security and free trade, governments could adopt an international "one key escrow" policy.[118] Supporters of the one key escrow policy argue that it would be efficient because it would reduce the transaction costs across international borders when investigating and prosecuting criminal behaviors.[119] Yet, others contend that adopting an international key escrow system would be too complex because it requires addressing many detailed and complicated questions, such as, the extent to which one country's law enforcement officers can act in another country, and in what situations evidence obtained abroad can be used domestically.[120]

C. WAPI: THE CHINESE ENCRYPTION STANDARD

Every country has its own rules of encryption, and China is no exception. China has restrictions on the import and use of encryption, but not on its export.[121] According to an article in 2004, Chinese government officials maintain that the encryption restrictions are aimed at Chinese citizens, not foreign companies, but foreign companies can expect the Chinese government to request details about the encryption the companies use and to require companies to appoint a contact who can give the government encryption keys when the government requests.[122] In other words, if an encryption vendor encrypts data in China, the vendor would have to provide the Chinese government with the ability to access the keys.[123]

With its accession into the World Trade Organization ("WTO") in 2001, China agreed to accept the obligations of the WTO's Agreement on Technical Barriers to Trade, which establishes "procedures for the

---

[118] "Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party, such as government may gain access to those keys to be able to view the contents of encrypted communications." Wikipedia, Key Escrow, http://en.wikipedia.org/wiki/Key_escrow (last visited Feb. 7, 2009).

[119] Burch, *supra* note 108.

[120] JON M. PEHA, ENCRYPTION POL'Y ISSUES 4 (1998), http://www.ece.cmu.edu/~peha/encrypt.pdf.

[121] Messmer, *supra* note 109.

[122] *Id.*

[123] *Id.*

development and implementation of voluntary product standards, mandatory technical regulations and certification procedures." [124] Although some U.S. government agencies and business interests have agreed that China has made progress in its trade practices, the U.S.-China Business Council, the principal organization of U.S. corporations engaged in business with China, claims that for some sectors, China's commitments are not clearly fulfilled. [125] China's unique requirements that depart from international standards are most often seen as an attempt to give Chinese companies an advantage in growing industries, such as encryption technology, by promoting its own exclusive standard.[126]

When the former Ministry of Information Industry of China[127] attempted to establish a new wireless standard, the encryption dispute between China and foreign companies burst out like a storm. By announcing its new Chinese-made encryption standard, WAPI, China required that the foreign computer and chip producers that wished to sell Wi-Fi[128] devices in China use Chinese encryption software and co-produce their goods with designated Chinese companies beginning on June 1, 2004.[129] Otherwise, the companies would be banned from the Chinese market, which is the world's second-largest personal

---

[124] Susan Krause, *China's Industrial Policies Conflict with WTO Rules, Experts Say*, WASH. FILE, June 2, 2005, http://usinfo.org/wf-archive/2005/050602/epf407.htm.

[125] *Id.*

[126] *See* Bruce Einhorn, *China's Wi-Fi Wrangle*, BUSINESSWEEK, Mar. 15, 2004, http://www.businessweek.com/technology/content/mar2004/tc20040315_6034_tc058.htm; *see* Adam Segal, *How to Persuade China to Trade Fairly*, FINANCIAL TIMES, Aug. 20, 2004, http://www.cfr.org/publication.html?id=7264.

[127] In March 2008, the Ministry of Information Industry changed its name to the Ministry of Industry and Information Technology. Wikipedia, Ministry of Industry and Information Technology, http://en.wikipedia.org/wiki/Ministry_of_Industry_and_Information_Technology (last visited Feb. 7, 2009).

[128] Wi-Fi (wireless fidelity), trademark of the Wi-Fi Alliance. The products of the organization are certified by the Wi-Fi Alliance and this certification warrants interoperability between wireless devices. Wikipedia, Wi-Fi, http://en.wikipedia.org/wiki/Wi-Fi (last visited Feb. 7, 2009).

[129] Steve Lohr, *Technology; U.S. Pressing China to Yield On Wireless Encryption*, N.Y. TIMES, Mar. 4, 2004, http://query.nytimes.com/gst/fullpage.html?res=9B0CE3DC133FF937A35750C0A9629C8B63.

computer market behind the United States.[130] Support for WAPI was not included in Wi-Fi Protected Access[131] or 802.11i,[132] an amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks, developed and enforced by IEEE and the Wi-Fi Alliance.[133] According to a notice given by the Standardization Administration of China, WAPI, a different security protocol, was to be used with Wi-Fi standards in the 2.4GHZ radio band.[134] Moreover, further confusion was expected in the market because WAPI added another security specification that companies would have to consider when they installed a Wi-Fi network.[135]

D. KEY ISSUES OF WAPI IN INTERNATIONAL TRADE

One major global issue that arose from the WAPI dispute was the concern of an unfair trade barrier to sales, and on this ground, foreign computer and chip makers (led by U.S. companies) strongly protested the plan.[136] Finding 802.11 as a global standard in the wireless arena, China appeared to be using its market and proprietary standard to leverage control of the wireless sector by requiring foreign companies

---

[130] *China's New Wireless Standard Met with Intel Resistance*, PEOPLE'S DAILY ONLINE, Mar. 12, 2004, http://english.peopledaily.com.cn/200403/12/print20040312_137342.html; Posting of Andrew, NBR Admin. and Reviewer, to Notebook News and Reviews, http://forum.notebookreview.com/showthread.php?t=738 (Mar. 14, 2004, 01:31 EST) (In 2003, China purchased more than 13 million PCs, thus, pulling the products off the Chinese market would mean huge losses for the companies.).

[131] Wi-Fi Protected Access is "a certification program administered by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks." Wikipedia, Wi-Fi Protected Access, http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access (last visited Feb. 7, 2009).

[132] For more information on IEEE 802.11, see Wikipedia, IEEE 802.11i-2004, http://en.wikipedia.org/wiki/802.11i (last visited Feb. 7, 2009).

[133] Richard Shim, *China to Adopt Own Wi-Fi Security Standard*, SILICON.COM, Dec. 3, 2003, http://networks.silicon.com/mobile/0,39024665,39117179,00.htm.

[134] *Id.*

[135] *Id.*

[136] Lohr, *supra* note 129; Kenneth Wong, *China Resolute on Standard as Intel Pulls Centrino*, BLOOMBERG.COM, Mar. 11, 2004, http://www.bloomberg.com/apps/news?pid=10000103&sid=aODZeayhUL.I&refer=us.

to manufacture WLAN products in China or to export them and partner with Chinese companies.[137] One analyst voiced criticism that China was creating trade barriers that impeded the import of semiconductors to unfairly favor its own chip industry.[138] Thus, many foreign companies and industry groups were concerned that WAPI could even fracture the WLAN equipment market because it is not compatible with the already existing WLAN encryption standards.[139] However, the response from the Chinese government to such criticisms was that the encryption standard was only for information security concerns and would make China's wireless networks safe for users.[140]

Another major issue is the "forced" licensing with Chinese companies. At the time of the announcement, only twenty-four Chinese companies held the encryption technique of the WAPI security standard.[141] Thus, under the new wireless standard, foreign companies had no choice but to cooperate with the twenty-four companies by licensing the WAPI protocol technology in order to get authorizations relating to the Chinese wireless technique.[142] This led to several concerns. First, licensing the technology through co-production agreements created apprehension of sharing proprietary technology with Chinese competitors, and presented a potential loss of intellectual property. [143] Second, the new standard would have imposed serious burdens on foreign companies who would have had to consider the cost of authentication, the expensive licensing royalties, and who would have been dependent on their Chinese competitors to

---

[137] Brown, *supra* note 102.

[138] Wong, *supra* note 136.

[139] Sumner Lemon, *No Compromise on WAPI as Intel's Barrett Heads to China*, INFOWORLD, Apr. 5, 2004, http://www.infoworld.com/article/04/04/05/HNbarrettochina_1.html; Jones, *supra* note 104 (examples of WLAN standards are the Wired Equivalency Protocol and Wireless Protected Access).

[140] Einhorn, *supra* note 126.

[141] *China's New Wireless Standard Met with Intel Resistance*, *supra* note 130.

[142] *Id.*; Messmer, *supra* note 109.

[143] Lemon, *supra* note 139.

obtain use of WAPI.[144] Third, the standard would have created burdens for both suppliers and users because, while 802.11 chip vendors, card makers, and infrastructure suppliers would need to produce two different products when delivering a new kit—one for China and one for the rest of the world—the enterprise users of 802.11 hardware would need to figure out how to upgrade their existing equipment.[145]

Some protests arose from a belief that the implementation of common international standards would allow technology to move faster into the marketplace and result in more innovation than multiple variations of the same technology.[146] The WAPI was an obvious attack on such support for the "common international standards" principle, as the Chinese government noted that it had deployed and implemented a technical-standards strategy to "break up [the] technical-standards monopoly imposed by developed countries in international trade."[147]

E. SETTLEMENT OF ENCRYPTION STANDARD DISPUTE AND ITS EFFECT

China's new encryption standard appeared to be a way for China to prevent manufacturers from entering its market, and as a result the U.S. government and U.S. technology companies lobbied China to change its decision on the mandatory use of WAPI, which became a point of trade friction between the United States and China.[148] In March 2004, the Bush administration sent a letter to the Chinese government pressuring China to abandon its plan on mandatory use of WAPI because such a standard, in the Bush administration's view, was an unfair barrier to trade.[149] About a month after the letter was

---

[144] *China's New Wireless Standard Met with Intel Resistance*, *supra* note 130; Messmer, *supra* note 109.

[145] Jones, *supra* note 104.

[146] Lemon, *supra* note 139.

[147] Brown, *supra* note 102 (quoting 2002 CHINA SCIENCE AND TECHNOLOGY INDICATORS (Scientific and Technical Documents Publishing House, 2002)).

[148] Messmer, *supra* note 109; *see* Wong, *supra* note 136 (The U.S. Information Technology Industry Council, an organization that represents high-technology companies in trade issues, commented that the new Chinese standard "would infringe on intellectual property rights and disrupt the global business models of non-Chinese companies.").

[149] Lohr, *supra* note 129 (Three U.S. cabinet-level officers, Secretary of Commerce Donald L. Evans, Secretary of State Colin L. Powell, and U.S. Trade Representative Robert B.

sent, the Chinese Vice-Premier finally announced that China would indefinitely delay implementation of the new standard, and the dispute was settled in peace.[150]

Although the implementation of WAPI resulted in a failure, and the dispute settled relatively quickly, China's encryption standard dispute is an important global issue because it may have created a dangerous precedent for using government standards as a barrier to international trade.[151] The possible trend of China setting its own exclusive standards caused fears in the global technology market that China "could fragment the high-technology global markets in a misguided protectionist attempt to give Chinese producers an edge."[152] China promulgated this fear by continuing to fight for its exclusive WAPI standard until, in 2006, the Geneva-based International Standards Organization ("ISO") finally rejected China's WAPI system in favor of the widely used 802.11i encryption standard.[153]

In 2006, after the ISO members overwhelmingly rejected China's WAPI system as a global standard, China accused the IEEE of conspiracy against WAPI, and of "unethical activities," such as misleading national agencies by persuading them to reject the WAPI

Zoellick, expressed their concerns in a joint letter to deputy prime ministers in Beijing in an attempt to remove potential conflicts between China and the United States in high-technology trade. The letter was not released to the public but it was known to contain concerns focused on the wireless dispute and a broader concern about use of a technical standard as a trade barrier.).

[150] Shannon Feaster, *Chinese to Revise Unique WLAN Security Standard*, INFO. TECH. INDUS. COUNCIL, Apr. 21, 2004, http://www.itic.org/archives/articles/20040421/chinese_to_revise_unique_wlan_security_standard.php (The Chinese decision was made after a high-level discussion between U.S. and Chinese officials at the U.S.-China Joint Commission on Commerce and Trade meeting.).

[151] Lemon, *supra* note 139.

[152] Lohr, *supra* note 129. China was also developing its own standards for video compression, digital television signals, and high-speed cell phone networks. Wong, *supra* note 136.

[153] *China, U.S. Spar Over Encryption*, WIRED, May 30, 2006, http://www.wired.com/print/science/discoveries/news/2006/05/71020; Elena Malykhina, *China Fights For Its Wireless Standard Against Intel-Backed 802.11i*, INFORMATIONWEEK, May 31, 2006, http://www.informationweek.com/news/management/showArticle.jhtml?articleID=188700275 (802.11i received approval by 89% of ISO members, while WAPI received 32%. The Chinese officials felt that the approval process was unfairly stacked against WAPI.).

standard.[154] Had China been successful in pushing its new encryption policy, China possibly could have implemented protectionist measures with respect to other technology, such as cell phones.[155] However, China's failure to achieve international acceptance of its WAPI wireless encryption standard appears to have led the former Ministry of Information Industry of China to recently approve the use of European and U.S. standards for 3G mobile phones.[156]

IV. CONCLUSION

China has grown to be an attractive destination for global trade. After entry into the WTO, China has been implementing measures to open its market and liberalize its trade practices.[157] While China has worked to open itself as a market for international trade, its lack of a privacy law indicates that it is not yet ready to protect the massive amount of information that flows in and out of the country on a daily basis. Similarly, regardless of the criticism that the unique Chinese encryption standard was a disguised trade barrier, China's stubborn insistence on its own encryption standard over international objections indicates that China has not completely modernized its trade practices. Accordingly, many fear that China's entry into the WTO is not about their interest in a level playing field, but rather, an easy way to earn global credibility and trade leverage.[158] Therefore, in order to promote global trade, China should prepare an adequate privacy framework and fair encryption standard that would appropriately balance its culture, economy, and legal structure with global standards.

---

[154] *China, U.S. Spar Over Encryption*, *supra* note 153; Malykhina, *supra* note 153.

[155] Einhorn, *supra* note 126 (quoting Anne Stevenson-Yang, managing director of the U.S. Information Technology Office in Beijing) (The new standard rule could also have been applied to imports of other devices, including cell phones, personal digital assistants, scanners, and network cards.).

[156] Rupert Goodwins, *China Gives the Nod to Western 3G Standards*, SILICON.COM, May 18, 2007, http://networks.silicon.com/mobile/0,39024665,39167188,00.htm.

[157] Krause, *supra* note 124.

[158] Brown, *supra* note 102.